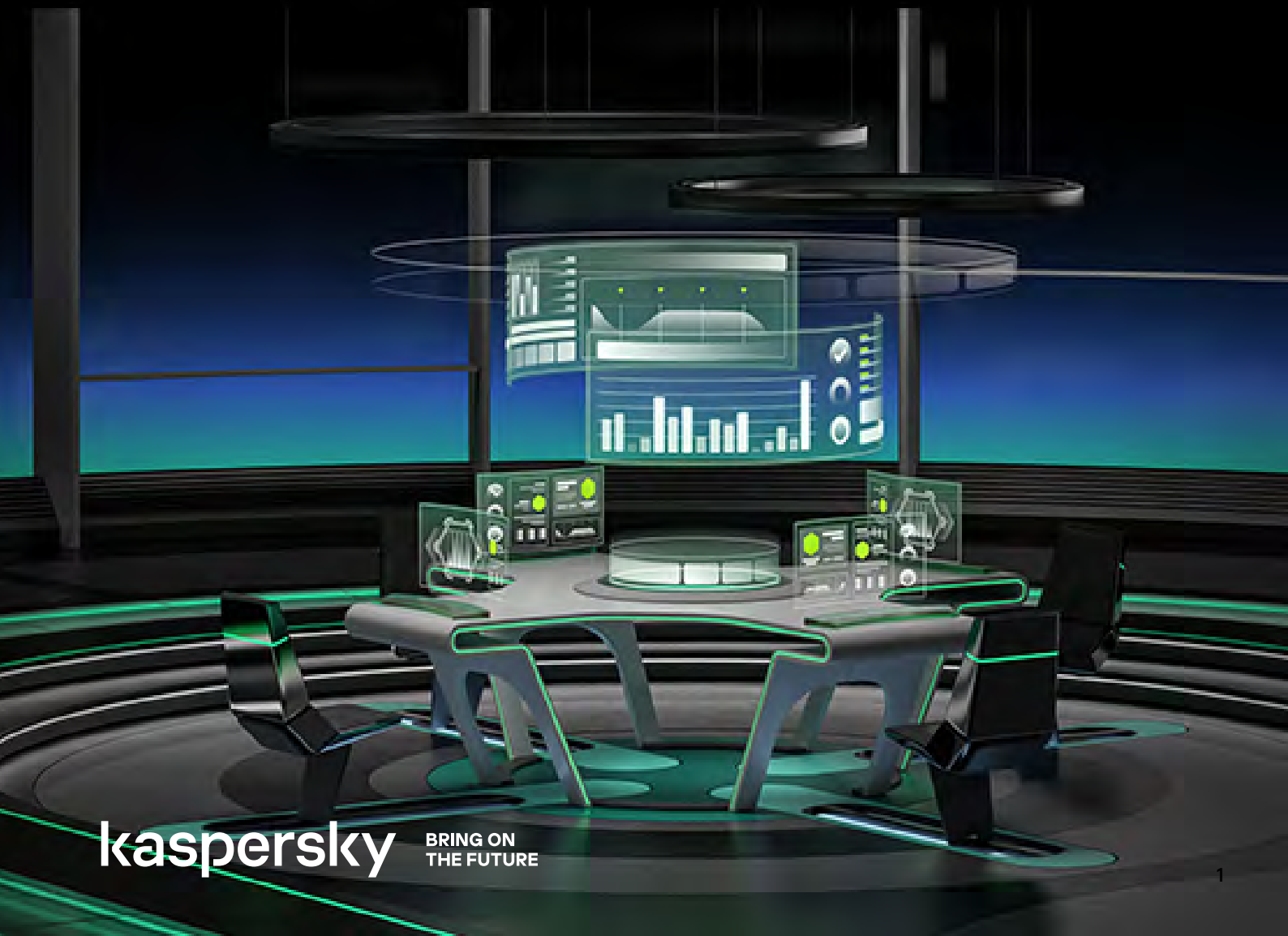
Kaspersky Security Bulletin 2021. Statistics



kaspersky BRING ON THE FUTURE

Contents

Figures of the year

- During the year, 15.45% of internet user computers worldwide experienced at least one **Malware-class** attack.
- Kaspersky solutions blocked **687,861,449** attacks launched from online resources across the globe.
- **114,525,734** unique malicious URLs triggered Web Anti-Virus components.
- Our Web Anti-Virus blocked **64,559,357** unique malicious objects.
- Ransomware attacks were defeated on the computers of **366,256** unique users.
- During the reporting period, miners attacked **1,184,986** unique users.
- Attempted infections by malware designed to steal money via online access to bank accounts were logged on the devices of **429,354** users.

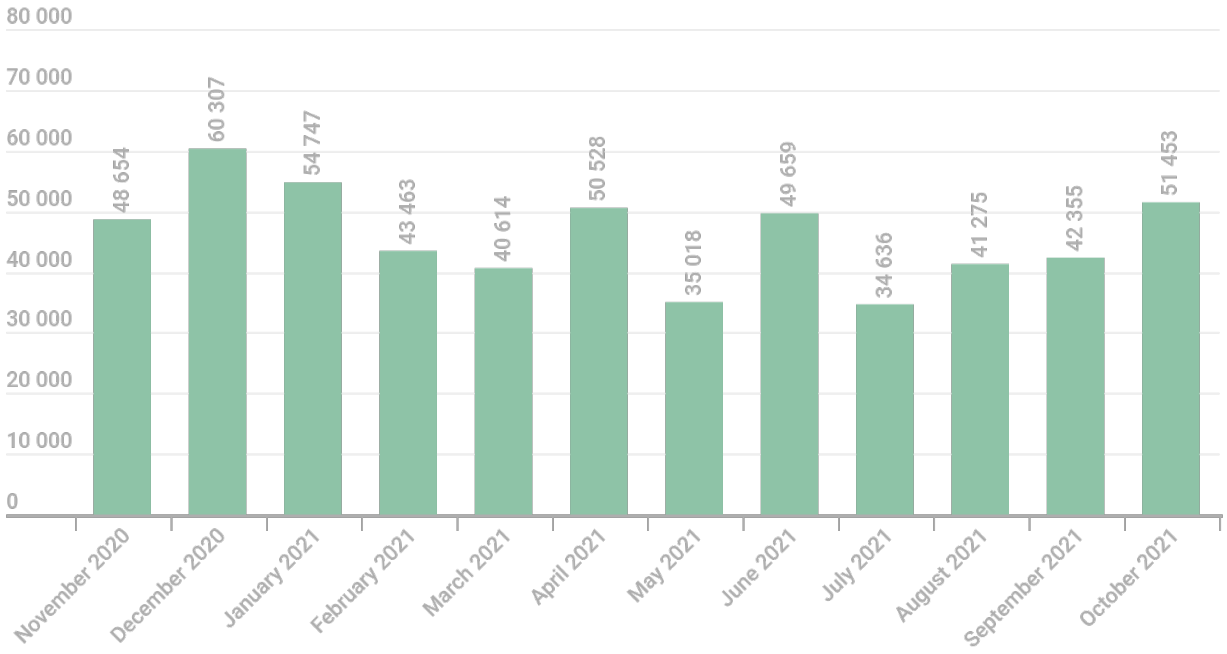
All statistics in this report are from the global cloud service Kaspersky Security Network (KSN), which receives information from components in our security solutions. The data was obtained from users who had given their consent to it being sent to KSN. Millions of Kaspersky users around the globe assist us in collecting information about malicious activity. The statistics in this report cover the period from November 2020 to October 2021, inclusive.

Financial threats

The statistics include not only banking threats, but also malware for ATMs and payment terminals. Statistics on analogous mobile threats are given in the separate report.

Number of users attacked by banking malware

During the reporting period, Kaspersky solutions blocked attempts to launch one or more malicious programs designed to steal money from bank accounts on the computers of **429,354** users.



Number of users attacked by financial malware, November 2020 — October 2021

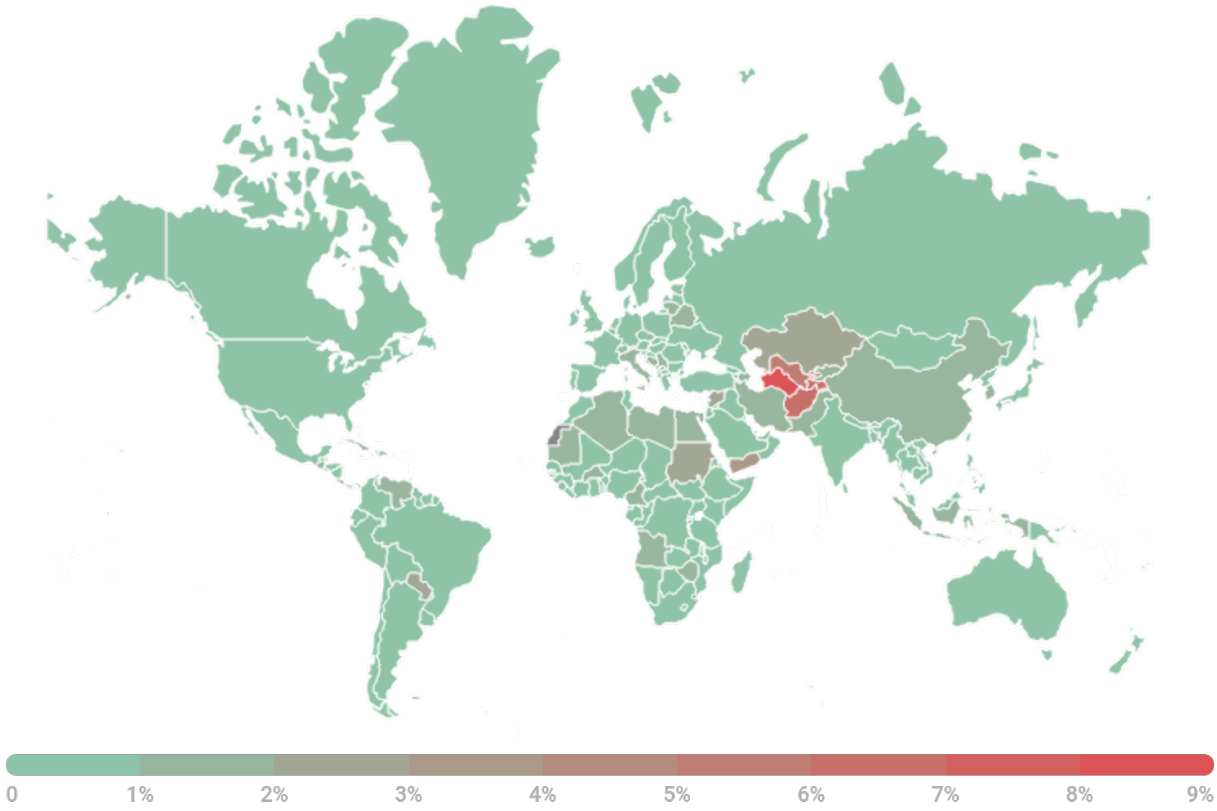
Top 10 financial malware families

	Name	Verdict	%*
1	Zbot	Trojan-Spy.Win32.Zbot	21.6
2	CliptoShuffler	Trojan-Banker.Win32.CliptoShuffler	12.7
3	SpyEye	Trojan-Spy.Win32.SpyEye	10.1
4	Trickster	Trojan.Win32.Trickster	4.7
5	RTM	Trojan-Banker.Win32.RTM	4.4
6	Nimnul	Trojan-Banker.Win32.Nimnul	3.7
7	Danabot	Trojan-Banker.Win32.Danabot	3.1
8	Cridex	Backdoor.Win32.Cridex	3.0
9	Nymaim	Trojan.Win32.Nymaim	2.1
10	Neurevt	Trojan.Win32.Neurevt	1.7

* Unique users attacked by this malware as a percentage of all users attacked by financial malware.

Attack geography

To evaluate and compare the risk of being infected by banking Trojans and ATM/POS malware worldwide, for each country we calculated the share of users of Kaspersky products who faced the financial threat during the reporting period as a percentage of all users of our products in that country who were attacked.



Geography of banking malware attacks, November 2020 — October 2021

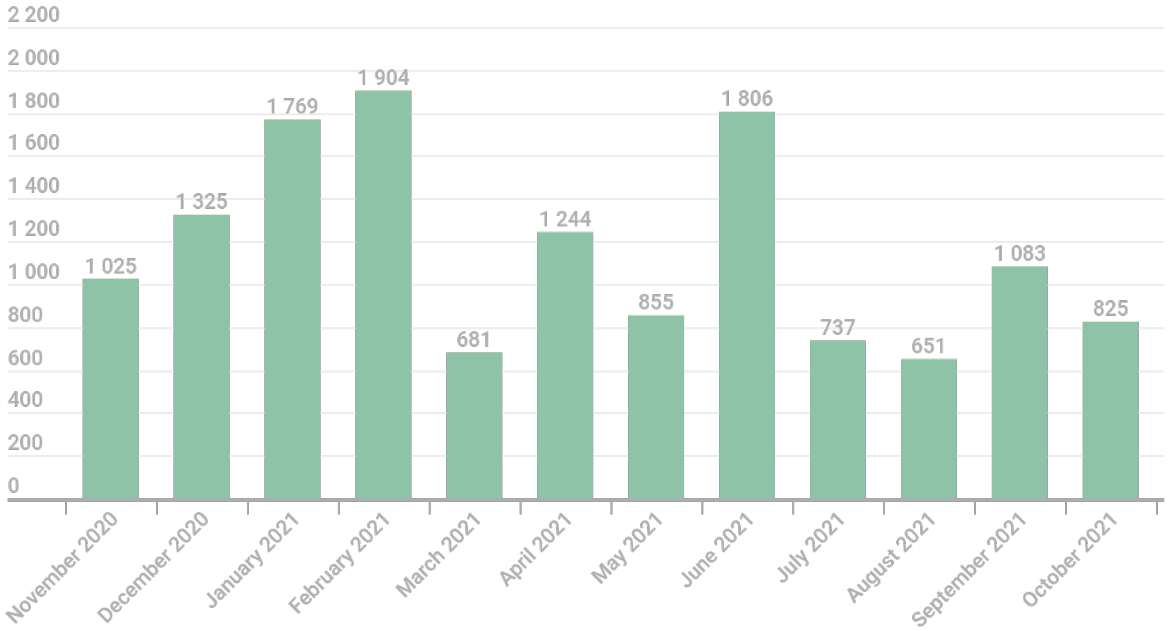
Top 10 countries by share of attacked users

	Country*	%**
1	Turkmenistan	8.4
2	Afghanistan	6.7
3	Tajikistan	6.6
4	Uzbekistan	5.7
5	Yemen	3.1
6	Paraguay	2.9
7	Costa Rica	2.7
8	Sudan	2.4
9	Kazakhstan	2.2
10	Syria	2.2

* Excluded are countries with relatively few Kaspersky product users (under 10,000).
** Unique users whose computers were targeted by financial malware as a percentage of all users attacked by all kinds of malware.

Ransomware programs

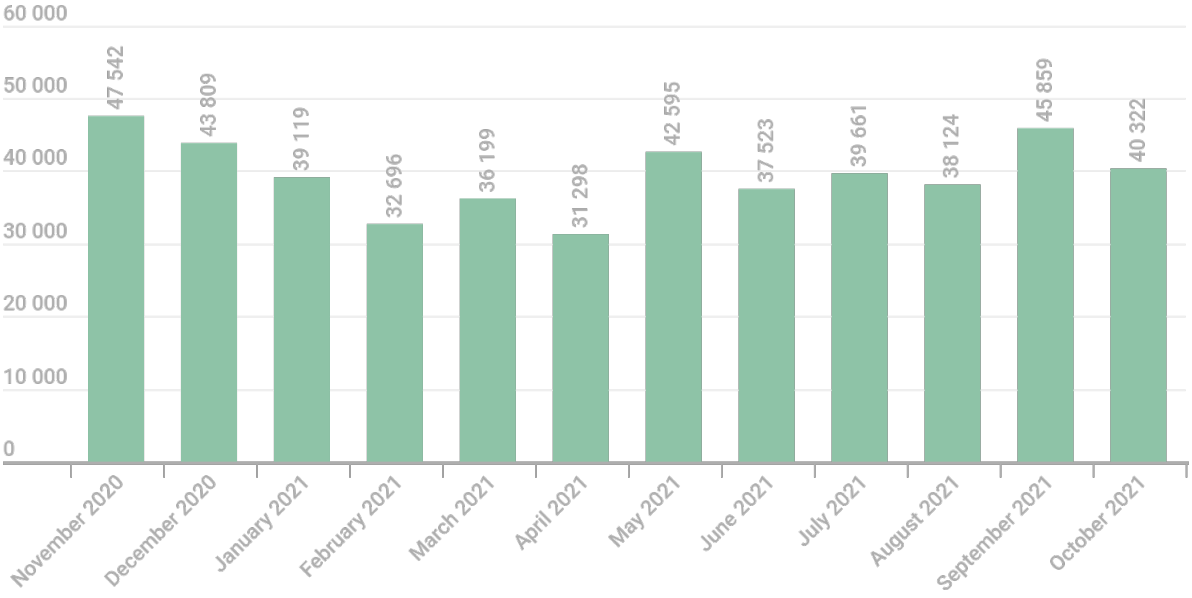
During the reporting period, we identified more than **13,905** ransomware modifications and detected **33** new families. Note that we did not create a separate family for each new piece of ransomware. Most threats of this type were assigned the generic verdict, which we give to new and unknown samples.



Number of new ransomware modifications detected, November 2020 — October 2021

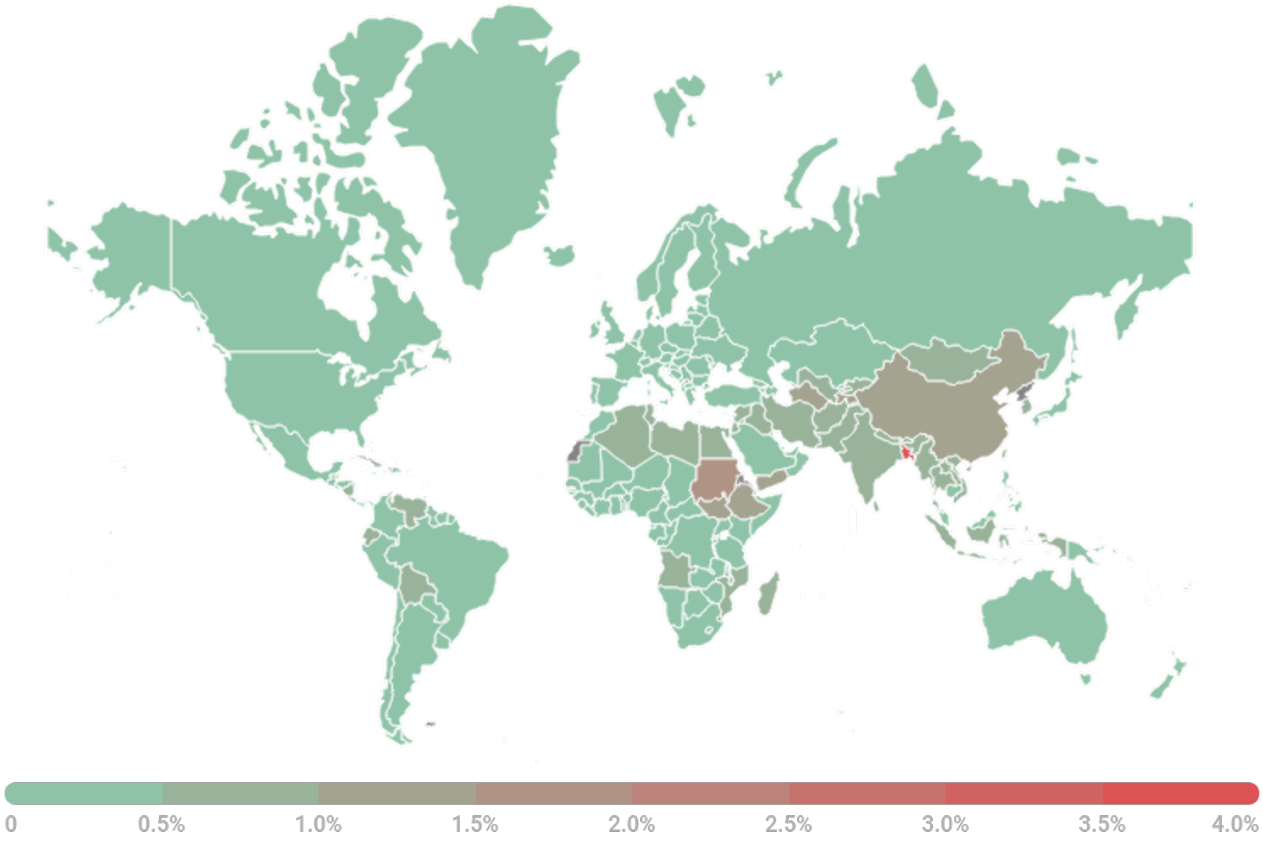
Number of users attacked by ransomware Trojans

During the reporting period, ransomware Trojans attacked **366,256** unique users, including **92,863** corporate users (excluding SMBs) and **12,699** users associated with small and medium-sized businesses.



Number of users attacked by ransomware Trojans, November 2020 — October 2021

Attack geography



Geography of attacks by ransomware Trojans, November 2020 — October 2021

Top 10 countries attacked by ransomware Trojans

	Country*	%**
1	Bangladesh	3.69
2	Haiti	1.79
3	Sudan	1.69
4	Turkmenistan	1.41
5	Palestine	1.33
6	Yemen	1.10
7	Tajikistan	1.03
8	China	1.01
9	Ethiopia	1.00
10	Pakistan	0.87

* Excluded are countries with relatively few Kaspersky users (under 50,000).
** Unique users whose computers were attacked by Trojan encryptors as a percentage of all unique users of Kaspersky products in the country.

Top 10 most common families of ransomware Trojans

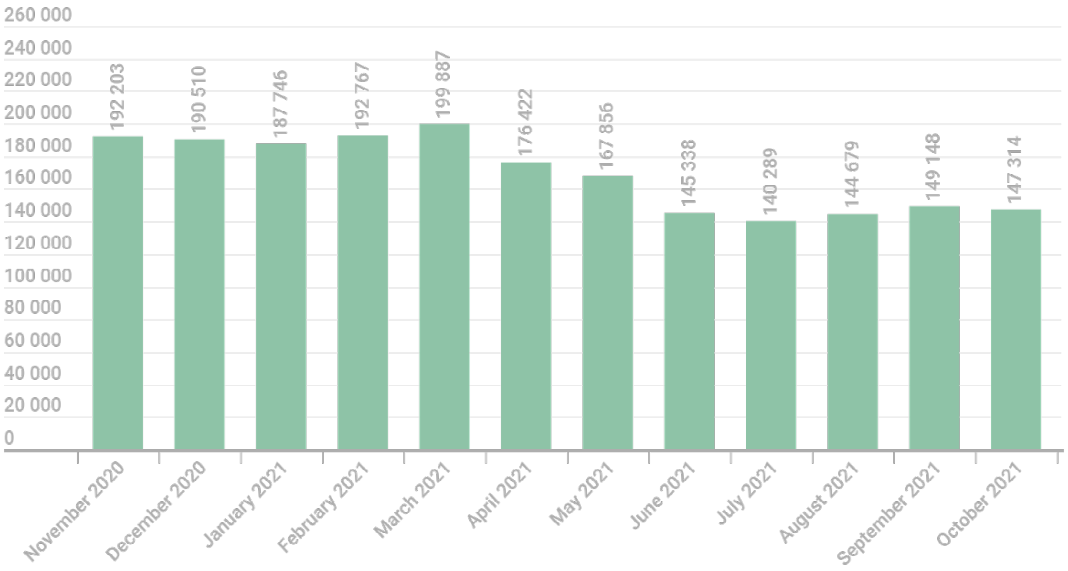
	Name	Verdict	%*
1	Stop/Djvu	Trojan-Ransom.Win32.Stop	17.30
2	WannaCry	Trojan-Ransom.Win32.Wanna	15.34
3	(generic verdict)	Trojan-Ransom.Win32.Gen	9.73
4	(generic verdict)	Trojan-Ransom.Win32.Crypren	9.31
5	(generic verdict)	Trojan-Ransom.Win32.Encoder	6.66
6	(generic verdict)	Trojan-Ransom.Win32.Phny	6.22
7	(generic verdict)	Trojan-Ransom.Win32.Agent	4.01
8	PolyRansom/VirLock	Virus.Win32.PolyRansom Trojan-Ransom.Win32.PolyRansom	2.72
9	(generic verdict)	Trojan-Ransom.Win32.Generic	1.57
10	(generic verdict)	Trojan-Ransom.Win32.Crypmod	1.40

* Kaspersky users attacked by a particular family of ransomware Trojans as a percentage of all users attacked by ransomware Trojans.

Miners

Number of users attacked by miners

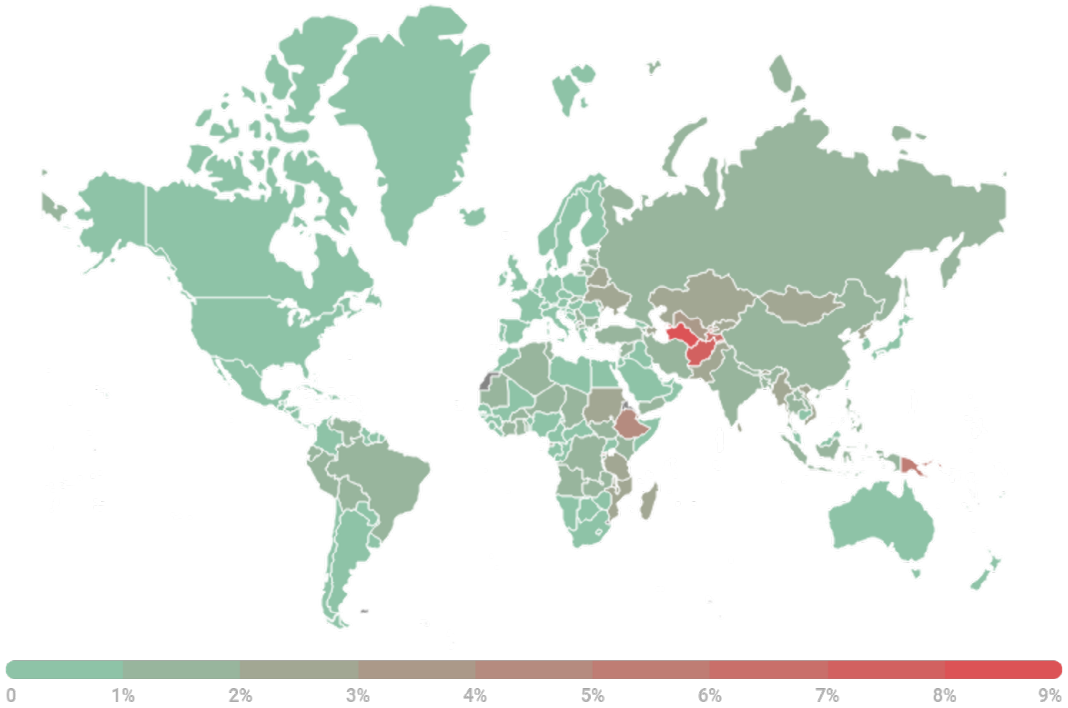
During the reporting period, we detected attempts to install a miner on the computers of **1,184,986** unique users. Miners accounted for 2.19% of all attacks and 16.88% of all Risktool-type programs.



Number of users attacked by miners, November 2020 — October 2021

During the reporting period, Kaspersky products detected Trojan.Win32.Miner.bbb more often than others, accounting for 20.73% of all users attacked by miners. It was followed by Trojan.Win32.Miner.gen (11.58%), Trojan.Win32.Miner.ays (8.73%) and Trojan.Win32.Miner.vogh (3.52%).

Attack geography



Geography of miner-related attacks, November 2020 — October 2021

Vulnerable applications used by cybercriminals during cyberattacks

Notably, most of the reporting period's zero-day vulnerabilities were detected during active exploitation by cybercriminals, including well-known APT groups. Throughout 2021, Kaspersky experts discovered several vulnerabilities, including:

- The vulnerability **CVE-2021-28310**, which we believe was exploited by the BITTER APT group. An out-of-bounds (OOB) write bug in Desktop Window Manager allows data to be written outside the memory buffer, enabling privilege escalation in the system. This allows attackers, for example, to break out of the sandbox if this vulnerability is exploited with some other vulnerability in the browser or other software. We have already detailed this CVE in a **separate report**.
- Two vulnerabilities (**CVE-2021-31955, CVE-2021-31956**) used in a chain of exploits as the second stage after exploitation of a vulnerability in the browser to break out of its sandbox. The first of these two vulnerabilities is an information leak, allowing an attacker to obtain the address of the EPROCESS structure in the kernel memory; the second uses a heap memory overflow bug in the NTFS driver to read and write arbitrary data in the kernel memory, which in turn can lead to privilege escalation in the system. A detailed technical description of both can be found in **our post**.
- **CVE-2021-40449**, used by an APT group in the MysterySnail operation, is a use-after-free vulnerability in the win32k driver. It reveals itself during the processing of user callback functions and ultimately delivers control over the attacked system. See **here** for our technical analysis of this vulnerability.

Our partners detected other attacks that exploited various vulnerabilities:

- Fourteen vulnerabilities in Google Chrome (**CVE-2021-21148, CVE-2021-21166, CVE-2021-21193, CVE-2021-21206, CVE-2021-30551, CVE-2021-30554, CVE-2021-30563, CVE-2021-30632, CVE-2021-30633, CVE-2021-37973, CVE-2021-37975, CVE-2021-37976, CVE-2021-38000, CVE-2021-38003**) were used by various cybercriminals to compromise attacked systems and run malicious code. Most of the vulnerabilities affected the V8 scripting engine and exploited bugs related to heap buffer overflow, race conditions and data type confusion, as well as use-after-free vulnerabilities in Blink, Audio and other components.
- Four remote code execution vulnerabilities were discovered in Microsoft Exchange Server (**CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065**). They allow attackers to gain control of mail servers that have not been duly patched.
- Four remote code execution vulnerabilities in Microsoft Internet Explorer (**CVE-2021-26411, CVE-2021-33742, CVE-2021-34448, CVE-2021-40444**) can be used to introduce malware into the target system through infected websites visited by the user.
- Two vulnerabilities (**CVE-2021-21017, CVE-2021-28550)** exploiting heap overflow and use-after-free bugs in Adobe Reader.
- Five vulnerabilities in the Microsoft Windows operating system itself (**CVE-2021-31199, CVE-2021-31201, CVE-2021-33771, CVE-2021-31979, CVE-2021-36948**) and one in Microsoft Windows Defender (**CVE-2021-1647**). These also allow an attacker to elevate system privileges.

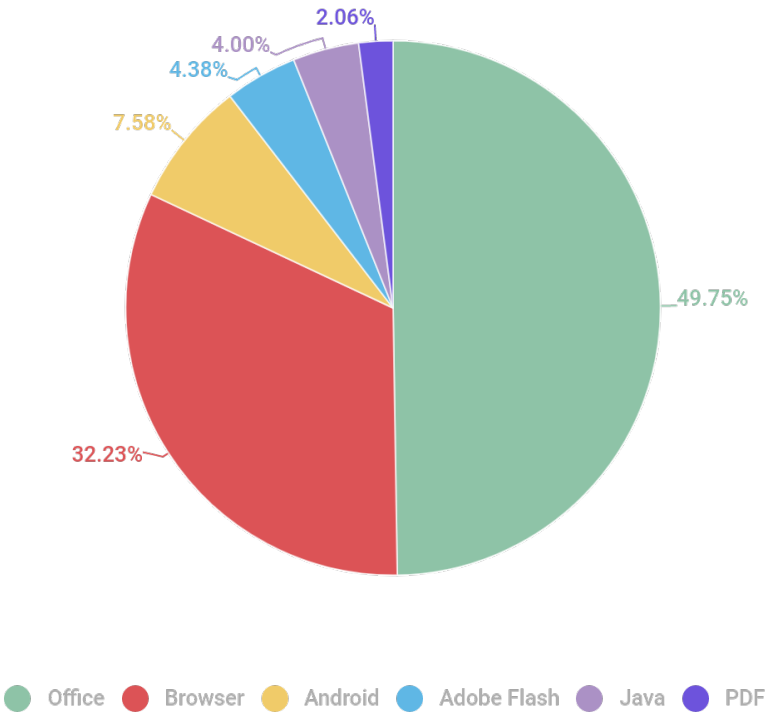
In the reporting period, we saw a downward trend in the number of exploitations of Microsoft Office vulnerabilities (-17.25 p.p.), although exploits for this software suite are still the most popular among cybercriminals, being the easiest way to compromise vulnerable user systems. Among the most frequently used CVEs are **CVE-2017-11882, CVE-2018-0802, CVE-2017-8570 and CVE-2017-0199**, which we have covered many times in previous posts. Also at the end of this year we have observed the newly discovered vulnerability **CVE-2021-40444**, active in the MSHTML engine of Internet Explorer and often exploited through a specially prepared Microsoft Office document with an embedded malicious ActiveX control for executing arbitrary code in the system. The emergence of public exploits for this vulnerability has spurred attempts to take advantage of it. See **our article** for details of CVE-2021-40444 exploitation.

Browser vulnerabilities are in second place in terms of popularity; in 2021 they were patched in succession by out-of-band security updates, while showing growth of 16.41 p.p. against the previous reporting period.

Third place in our statistics belongs to the Android platform, which lost 2.35 p.p. in the reporting period; the now obsolete Adobe Flash platform (+2.2 p.p.) lies in fourth place; Java is in fifth, while last place goes to vulnerabilities in PDF documents (+1.09 p.p.).

The rating of vulnerable applications is based on verdicts by Kaspersky products for blocked exploits used by cybercriminals both in network attacks and in vulnerable local apps, including on users' mobile devices.

The reporting period did not see any major changes to the statistics on exploitation of vulnerabilities in network services and components; bugs in software and OS components are still a common method to penetrate vulnerable systems. However, most of the new exploits in 2021 were published by researchers, not found in-the-wild during exploitation by attackers. For example, critical vulnerabilities were discovered in Windows server and user systems, and were widely publicized in the media under the names PrintNightmare, HiveNightmare/SeriousSAM and PetitPotam. Other headline finds include a string of exploits for Microsoft Exchange Server vulnerabilities (ProxyToken, ProxyLogon, ProxyShell). Lastly, we continued to detect brute-force attacks on various network services, in particular RDP, MS SQL and SMB. Exploits from the Equation Group for outdated and unpatched Microsoft Windows systems also remain popular, among which EternalBlue and EternalRomance stand out from the crowd.



Distribution of exploits used in attacks by type of application attacked, November 2020 — November 2021

Attacks on macOS

Among the most interesting finds during the reporting period were malware for Apple's MacBook with M1 processor, the new Convuster adware for macOS written in Rust, as well as new samples of the XCSSET Trojan, which infects projects in the Xcode development environment and steals data from browsers and other applications.

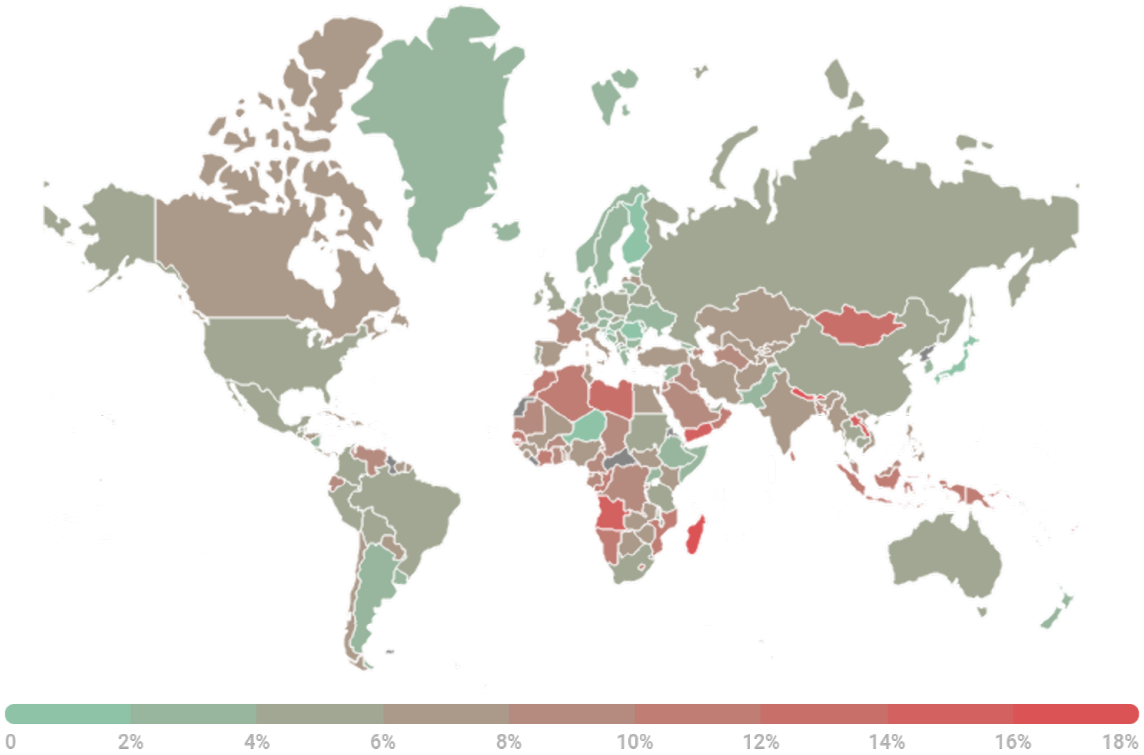
Top 10 threats for macOS

	Verdict	%*
1	AdWare.OSX.Pirrit.ac	14.44
2	AdWare.OSX.Pirrit.j	11.39
3	AdWare.OSX.Bnodlero.at	9.91
4	Trojan-Downloader.OSX.Shlayer.a	9.33
5	AdWare.OSX.Pirrit.gen	9.00
6	Monitor.OSX.HistGrabber.b	8.49
7	AdWare.OSX.Pirrit.o	8.28
8	AdWare.OSX.Pirrit.aa	7.60
9	Trojan-Downloader.OSX.Agent.h	6.38
10	AdWare.OSX.Bnodlero.t	6.27

* Unique users who encountered this malware as a percentage of all users of Kaspersky security solutions for macOS who were attacked.

Most of this reporting period's Top 10 was made up of adware. The Shlayer Trojan, which we wrote about back in early 2020, having ranked first in the last reporting period, dropped to fourth position.

Threat geography



Geography of threats for macOS, November 2020 — October 2021

Top 10 countries by share of attacked users

	Country*	%**
1	Ecuador	9.01
2	France	8.04
3	Spain	7.30
4	Vietnam	6.89
5	Canada	6.81
6	India	6.45
7	Italy	6.27
8	Turkey	6.19
9	United States	5.91
10	Mexico	5.60

* Excluded from the rating are countries with relatively few users of Kaspersky security solutions for macOS (under 5000).
** Unique users attacked as a percentage of all users of Kaspersky security solutions for macOS in the country.

IoT attacks

IoT threat statistics

During the reporting period, 77.47% of attacks on Kaspersky traps were carried out using the Telnet protocol.

Telnet	77.47%
SSH	22.53%

Distribution of attacked services by number of unique IP addresses of devices that carried out attacks, November 2020 — October 2021

As for distribution of sessions, Telnet also prevailed, accounting for more than two-thirds of all working sessions.

Telnet	71.33%
SSH	28.67%

Distribution of cybercriminal working sessions with Kaspersky traps, November 2020 — October 2021

Top 10 countries by location of devices from which attacks were carried out on Kaspersky Telnet traps

	Country*	%**
1	China	42.19
2	India	14.20
3	United States	5.07
4	Russia	4.22
5	Brazil	3.83
6	Vietnam	2.69
7	Taiwan, Province of China	2.02
8	Egypt	1.96
9	Iran	1.92
10	South Korea	1.47

* Devices from which attacks were carried out in the given country as a percentage of the total number of devices in that country.

Threats loaded into traps

	Verdict	%*
1	Backdoor.Linux.Mirai.b	48.25
2	Trojan-Downloader.Linux.NyaDrop.b	13.57
3	Backdoor.Linux.Mirai.ba	6.54
4	Backdoor.Linux.Gafgyt.a	5.51
5	Backdoor.Linux.Agent.bc	4.48
6	Trojan-Downloader.Shell.Agent.p	2.54
7	Backdoor.Linux.Gafgyt.bj	1.85
8	Backdoor.Linux.Mirai.a	1.81
9	Backdoor.Linux.Mirai.cw	1.52
10	Trojan-Downloader.Shell.Agent.bc	1.36

* Share of malware type in the total number of malicious programs downloaded to IoT devices following a successful attack.

Attacks via web resources

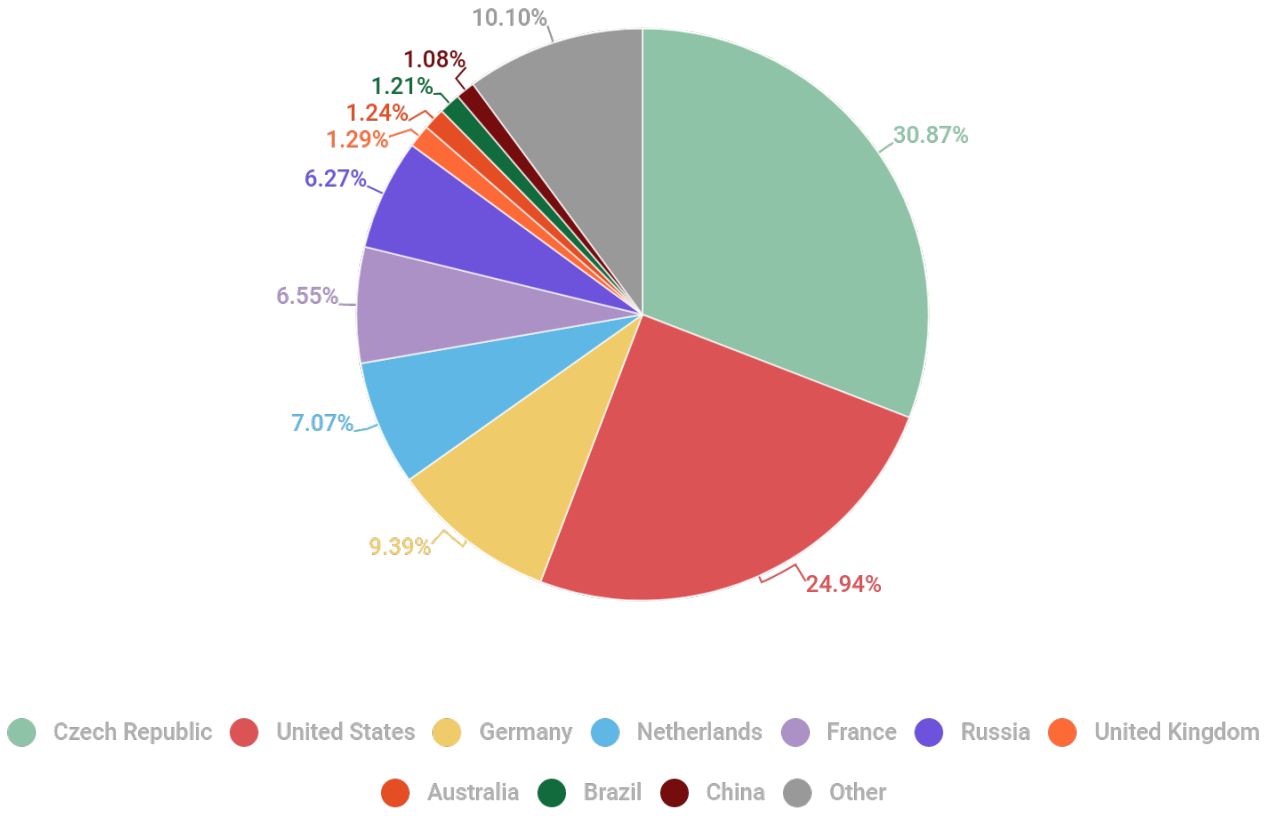
The statistics in this section are based on Web Anti-Virus, which protects users when malicious objects are downloaded from malicious/infected web pages. Cybercriminals create malicious websites on purpose; web resources with user-created content (for example, forums), as well as hacked legitimate resources, can be infected.

Countries that serve as sources of web-based attacks

The following statistics show the distribution by country of the sources of Internet attacks blocked by Kaspersky products on user computers (web pages with redirects to exploits, sites containing exploits and other malicious programs, botnet C&C centers, etc.). Any unique host could be the source of one or more web-based attacks.

To determine the geographical source of web-based attacks, domain names are matched against their actual domain IP addresses, and then the geographical location of a specific IP address (GEOIP) is established.

In the reporting period, Kaspersky solutions blocked **687,861,449** attacks launched from online resources across the globe. Moreover, 89.9% of these resources were located in just 10 countries.



Distribution of web attack sources by country, November 2020 — October 2021

The Czech Republic (30.87%) took first place in the reporting period. After topping the leaderboard last year, the US (24.94%) moved down to second position. Germany took bronze (9.39%).

Countries where users faced the greatest risk of online infection

To assess the risk of online infection faced by users in different countries, for each country we calculated the percentage of Kaspersky users on whose computers Web Anti-Virus was triggered during the quarter. The resulting data provides an indication of the aggressiveness of the environment in which computers operate in different countries.

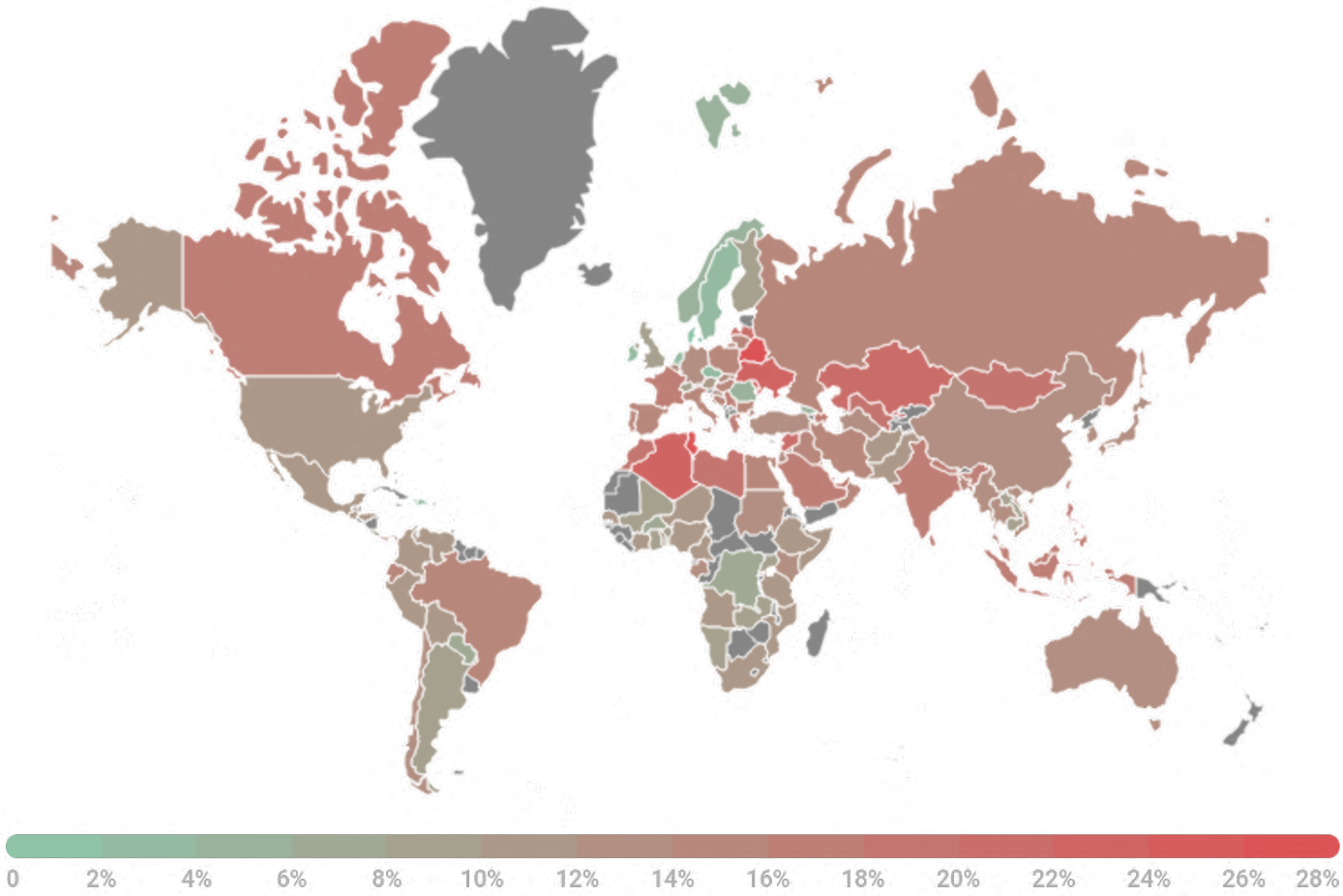
This rating only includes attacks by malicious objects that fall under the Malware class; it does not include Web Anti-Virus triggers in response to potentially dangerous or unwanted programs, such as RiskTool or adware. Overall, during the reporting period, adware and its components were registered on **78%** of users' computers on which the Web Anti-Virus was triggered.

Top 20 countries where users faced the greatest risk of online infection

	Country*	%**
1	Belarus	27.98
2	Tunisia	27.82
3	Algeria	23.76
4	Ukraine	23.70
5	Moldova	23.49
6	Latvia	20.95
7	Kazakhstan	20.64
8	Syria	20.32
9	Uzbekistan	19.77
10	Morocco	18.87
11	Qatar	18.69
12	Libya	18.46
13	Mongolia	18.36
14	Palestine	18.08
15	Serbia	17.99
16	Greece	17.73
17	Saudi Arabia	17.57
18	France	17.51
19	Nepal	17.41
20	Sri Lanka	17.30

* Excluded are countries with relatively few Kaspersky users (under 50,000).
** Unique users targeted by Malware-class attacks as a percentage of all unique users of Kaspersky products in the country.

On average, **15.45%** of internet user computers worldwide experienced at least one Malware-class attack during the reporting period.



Geography of malicious web-based attacks, November 2020 — October 2021

Top 20 malicious programs most actively used in online attacks

During the reporting period, Kaspersky's Web Anti-Virus detected **64,559,357** unique malicious objects (scripts, exploits, executable files, etc.), as well as **114,525,734** unique malicious URLs on which Web Anti-Virus was triggered. Based on the collected data, we identified the 20 most actively used malicious programs in online attacks on user computers.

In the reporting period, the share of adware and its components accounted for 91% of the total number of triggerings of our Web Anti-Virus on user computers.

	Verdict*	%**
1	Malicious URL	64.13
2	Trojan.Script.Generic	5.79
3	Trojan.BAT.Miner.gen	5.52
4	Trojan.Script.Miner.gen	5.51
5	Trojan.Multi.Preqw.gen	3.73
6	Trojan.Script.Agent.dc	2.59
7	Hoax.HTML.FraudLoad.m	1.60
8	Trojan.PDF.Badur.gen	1.23
9	Trojan-Downloader.Script.Generic	0.95
10	Backdoor.HTTP.TeviRat.gen	0.41
11	Exploit.MSOffice.CVE-2017-11882.gen	0.38
12	DangerousObject.Multi.Generic	0.37
13	Trojan-Downloader.JS.Agent.oms	0.35
14	Trojan-PSW.Script.Generic	0.34
15	Exploit.Win32.CVE-2011-3402.a	0.26
16	Exploit.Script.CVE-2021-26855.e	0.17
17	Trojan.MSOffice.SAgent.gen	0.16
18	Hoax.Script.FakeTechnicalSupport.gen	0.16
19	Trojan-Downloader.MSOffice.SLoad.gen	0.14
20	Trojan.Script.Agent.gen	0.14

* Excluded from the list are HackTool-type threats.

** Attacks by the given malicious program as a percentage of all Malware-class web attacks registered on the computers of unique users of Kaspersky products.

Local threats

Statistics on local infections of user computers is an important indicator. They include objects that penetrated the target computer through infecting files or removable media, or initially made their way onto the computer in non-open form (for example, programs in complex installers, encrypted files, etc.). These statistics additionally include objects detected on user computers after the first system scan by Kaspersky's Anti-Virus application.

This section analyzes statistics produced by Anti-Virus scans of files on the hard drive at the moment they were created or accessed, as well as the results of scanning removable storage media.

Top 20 malicious objects detected on user computers

We identified the 20 most commonly detected threats on user computers during the reporting period. Not included are Riskware-type programs and adware.

	Verdict*	%**
1	DangerousObject.Multi.Generic	23.94
2	Trojan.Multi.BroSubsc.gen	21.47
3	Trojan.Script.Generic	8.66
4	Trojan.Multi.GenAutorunReg.a	6.13
5	Trojan.Multi.Misslink.a	5.91
6	Trojan.Win32.SEPEH.gen	2.94
7	Trojan.WinLNK.Agent.gen	2.44
8	Exploit.Script.Generic	2.11
9	Trojan.Win32.Generic	1.89
10	Trojan.Win32.Agent.gen	1.86
11	Virus.Win32.Pioneer.cz	1.66
12	Trojan.WinLNK.Starter.gen	1.63
13	Hoax.Win32.DriverToolKit.b	1.59
14	Trojan.Win32.AutoRun.gen	1.59
15	Trojan.WinLNK.Runner.jo	1.54
16	Trojan.Script.Agent.gen	1.43
17	Trojan.BAT.Miner.gen	1.35
18	Worm.Python.Agent.c	1.30
19	Trojan.Multi.GenBadur.gen	1.29
20	Trojan.Win32.Agentb.bqyr	1.28

* Excluded from the list are HackTool-type threats.

** The share of unique users on whose computers File Anti-Virus detected the given object in the total number of unique users of Kaspersky products whose Anti-Virus was triggered by malware.

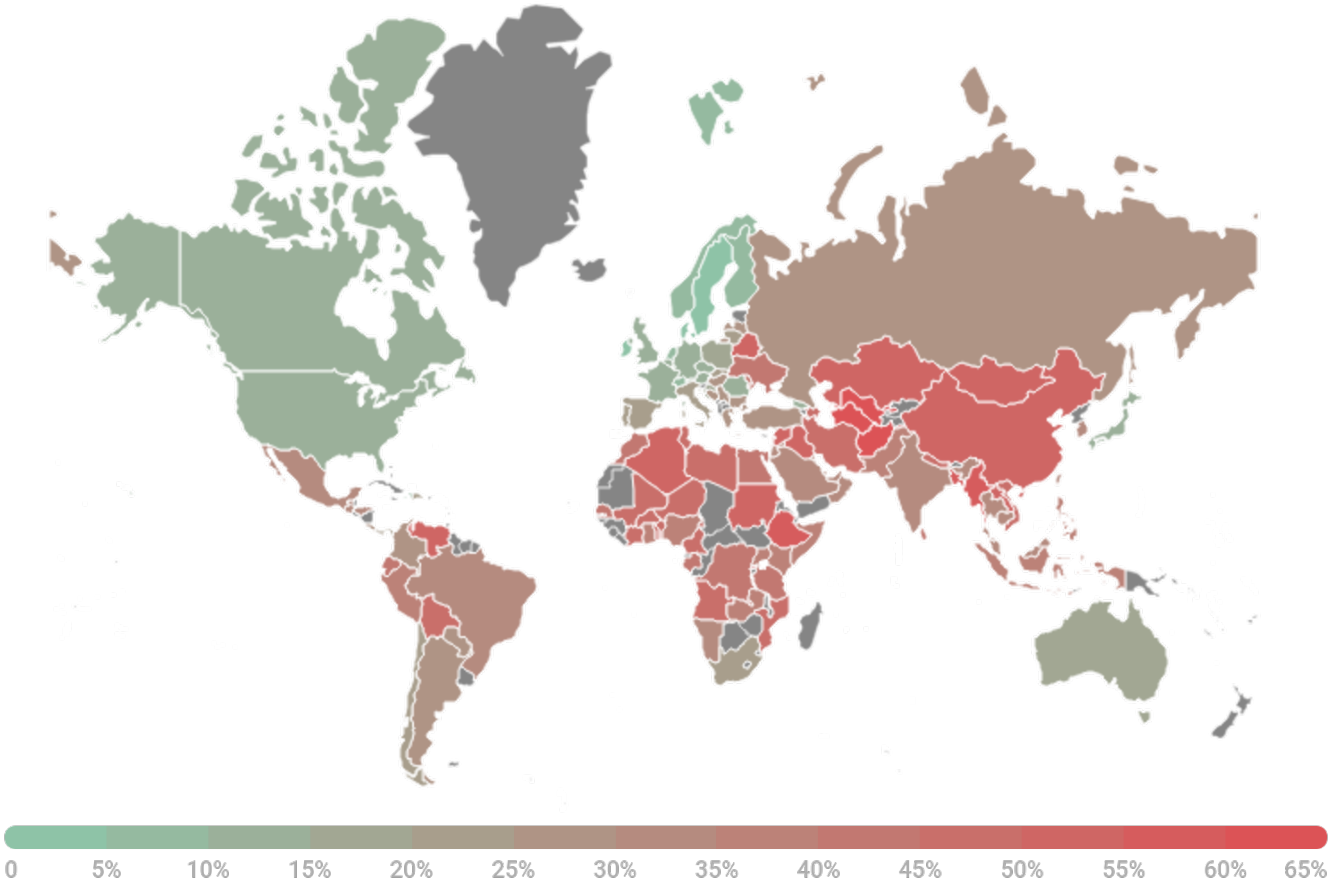
Countries where users faced the highest risk of local infection

For each country, we calculated how often users there encountered a File Anti-Virus triggering during the year. Included are detections of objects found on user computers or removable media connected to them (flash drives, camera/phone memory cards, external hard drives). These statistics reflect the level of personal computer infection in different countries.

Top 20 countries by level of risk of local infection

	Country*	%**
1	Turkmenistan	63.71
2	Uzbekistan	63.33
3	Afghanistan	62.67
4	Ethiopia	57.70
5	Myanmar	57.03
6	Bangladesh	55.64
7	Algeria	53.61
8	Venezuela	53.44
9	Iraq	52.79
10	Belarus	52.38
11	Laos	52.20
12	Syria	52.16
13	China	51.99
14	Sudan	50.80
15	Mongolia	50.29
16	Rwanda	50.23
17	Kazakhstan	50.07
18	Benin	49.48
19	Libya	49.16
20	Vietnam	49.04

* Excluded are countries with relatively few Kaspersky product users (under 50,000).
** Unique users on whose computers Malware-class local threats were blocked, as a percentage of all unique users of Kaspersky products in the country.



**Geography of local infections by malware,
November 2020 — October 2021**

During the reporting period, on average, at least one piece of malware was detected on **29.15%** of computers, hard drives or removable media belonging to users of Kaspersky solutions.